Claims

[c1] A method for preventing intrusion in a communications network having a plurality of nodes, comprising the steps of:

initiating a request for network services by a source node;

constructing a transformed packet header and transmitting a synchronization packet with the transformed packet header to a destination node;

authenticating the received packet by examination of the transformed packet header;

releasing the authenticated packet to the destination node; and

reforming the transformed packet header at the destination node.

[c2] The method for preventing intrusion in a communications network of claim 1 further comprising the step of transmitting an acknowledgement response with a transformed packet header to the source node.

[c3] The method for preventing intrusion in a communications network of claim 1 wherein the request for network services is a request for a session connection with the destination node.

[c4] The method for preventing intrusion in a communications network of claim 1 further comprising the step of authenticating a source identification by comparing a previously stored value with the source identification value determined for the source node.

[c5] The method for preventing intrusion in a communications network of claim 4 wherein the previously stored value and the determined source identification value are based on a hardware address of the source node and an associated user identification.

[c6] The method for preventing intrusion in a communications network of claim 4 wherein the request for network services is terminated if the determined source identification value does not match the previously stored value.

[c7] The method for preventing intrusion in a communications network of claim 6 further comprising the step of reporting the termination of the request for

network services in a message to a network administrator and storing the message in an unauthorized event database.

[c8] The method for preventing intrusion in a communications network of claim 1 wherein the step of constructing a transformed packet header comprises the steps of:

selecting a key index value from a first array of key index values;

applying the selected first array key index value to transform a user identification;

appending the first array key index value to the transformed user identification;

selecting a key index value from a second array of index values;

applying the second array key index value to the transformed user identification and appended first array key index value to form a first packet header field; and

storing the first packet header field in a transmit buffer.

[c9] The method for preventing intrusion in a communications network of claim 8 wherein the step of constructing a transformed packet header further comprises the steps of:

appending the second array key index value to a determined source identification value to form a resulting source identification value;

applying a transformation routine to the resulting source identification value to form a second packet header field; and

storing the second packet header field in the transmit buffer.

[c10] The method for preventing intrusion in a communications network of claim 1 further comprising the steps of:

inspecting each received packet to determine a corresponding transport protocol;

inspecting each received packet matching a selected protocol type to determine if the received packet is a synchronization packet;

retaining the received packet for further processing if the received packet is a synchronization packet.

[c11] The method for preventing intrusion in a communications network of claim 10 further comprising the step of releasing the received packet if it does not match a selected protocol type.

[c12] The method for preventing intrusion in a communications network of claim 10 further comprising the step of releasing the received packet if it is not a synchronization packet.

[c13] The method for preventing intrusion in a communications network of claim 1 wherein the step of authenticating the received packet comprises the steps of:

determining if the received packet originated from a trusted source node; and

executing an exception module if the received packet originated from an untrusted source node.

[c14] The method for preventing intrusion in a communications network of claim 1 wherein the step of authenticating the received packet comprises the steps of:

determining if the received packet originated from a trusted source node;

examining the packet header of the received packet to determine if the packet header has been transformed by the source node;

extracting a determined source identification value and an associated source user identification from the transformed packet header; and

inspecting the packet header to determine if an access policy is specified for the source node.

[c15] The method for preventing intrusion in a communications network of claim 14 further comprising the steps of determining if a hardware policy is defined and identifying the source node requesting the network services.

[c16] The method for preventing intrusion in a communications network of claim 14 further comprising the steps of determining if an application policy is defined and verifying a destination port.

[c17] The method for preventing intrusion in a communications network of claim 14 further comprising the steps of determining if a destination policy is defined and verifying a destination port.

[c18] The method for preventing intrusion in a communications network of claim 14 further comprising the step of terminating the request for network services if either no access policy is specified or if the specified access policy cannot be verified.

[c19] The method for preventing intrusion in a communications network of claim 18 further comprising the step of reporting the termination of the request for network services in a message to a network administrator and storing the message in an unauthorized event database.

[c20] The method for preventing intrusion in a communications network of claim 1 further comprising the step performed at the destination node of inspecting each received packet to determine if the received packet is a synchronization packet.

[c21] The method for preventing intrusion in a communications network of claim 20 further comprising the step of examining the packet header to determine if the packet header has been transformed by the source node.

[c22] The method for preventing intrusion in a communications network of claim 21 further comprising the steps of terminating the request for network services, reporting the termination of the request for network services in a message to a network administrator and storing the message in an unauthorized event database.

[c23] The method for preventing intrusion in a communications network of claim 1 wherein the step of reforming the transformed packet header comprises the steps of:

extracting a key index value from a packet header field; and

storing the key index value in a first buffer for use throughout a communications session between the source node and the destination node.

[c24] The method for preventing intrusion in a communications network of claim 23 wherein the step of reforming the transformed packet header further comprises the steps of:

using the key index value to reform another packet header field; and storing a value resulting from the reformed another packet header field in a transmit buffer.

[c25] The method for preventing intrusion in a communications network of claim 24 further comprising the steps of setting the packet header field to a zero value and storing the zero value in the packet header field in the transmit buffer.

[c26] The method for preventing intrusion in a communications network of claim 25 further comprising the steps of applying the key index value to the packet header field and the another packet header field to transform the packet header.

[c27] The method for preventing intrusion in a communications network of claim 1 further comprising the steps performed at the destination node after a communications session is established with a source node:

receiving a packet at the destination node;

reforming a first packet header field using a previously stored key index value;

storing the reformed first packet header field in a receive buffer;

reforming a second packet header field using the key index value;

storing the reformed packet header filed in the receive buffer; and

processing the received packet with reformed first and second packet header fields.

[c28] The method for preventing intrusion in a communications network of claim 27 further comprising the steps of:

transforming the first and second reformed packet header fields;

storing the transformed first and second packet header fields in a transmit buffer; and

transmitting a response packet to the source node including the transformed first and second packet header fields.

[c29] The method for preventing intrusion in a communications network of claim 13 wherein the step of executing an exception routine comprises the steps of:

extracting an address of the source node from a network layer header of the received packet;
determining if the source node address is an address known to the communications network;
extracting an address of the destination node from a network layer header of the received packet;
determining if the destination node address is an address known to the communications network;
extracting a port number of the destination node from a transport layer header of the received packet; and
determining if the destination port number is known to the communications network.

[c30] The method for preventing intrusion in a communications network of claim 29 wherein the request for network services is terminated if any one of the source node address, the destination node address and the destination port number are not known to the communications network.

[c31] The method for preventing intrusion in a communications network of claim 29 wherein the step of executing an exception routine further comprises the steps of:

generating an initial value for a packet header field;
selecting a key index value from an array of key index values;
appending the key index value to the generated initial value;
applying the key index value to the generated initial value and appended key index value to form a new transformed packet header field; and
reassembling the received packet including the new transformed packet header field.

[c32] The method for preventing intrusion in a communications network of claim 31 further comprising the step of determining a checksum value for the new transformed packet header before releasing the received packet to the destination node.

[c33] A method for providing trusted communications between a source device and a

destination device in a communications network, comprising the steps of:

initiating a request for a communications session at the source device;

constructing a transformed packet header and transmitting a synchronization packet including the transformed packet header to the destination device;

receiving the synchronization packet at the destination device;

reforming the transformed packet header at the destination device; and

constructing a transformed packet header and transmitting an acknowledgement response including the transformed packet header to the source device.

[c34] The method for providing trusted communications of claim 33 further comprising the step of authenticating a source identification at the source device by comparing a previously stored value with a source identification value determined for the source device.

[c35] The method for providing trusted communications of claim 34 wherein the previously stored value and the determined source identification value are based on a hardware address of the source device and an associated user identification.

[c36] The method for providing trusted communications of claim 34 wherein the request for a communications session is terminated if the determined source identification value does not match the previously stored value.

[c37] The method for providing trusted communications of claim 36 further comprising the step of reporting the termination of the request for a communications session in a message to a network administrator and storing the message in an unauthorized event database.

[c38] The method for providing trusted communications of claim 33 wherein the step of constructing a transformed packet header comprises the steps of:

selecting a key index value from a first array of key index values;

applying the selected first array key index value to transform a user identification;

appending the first array key index value to the transformed user identification;

selecting a key index value from a second array of index values;

applying the second array key index value to the transformed user identification and appended first array key index value to form a first packet header field; and

storing the first packet header field in a transmit buffer.

[c39] The method for providing trusted communications of claim 38 wherein the step of constructing a transformed packet header further comprises the steps of:

appending the second array key index value to a determined source identification value to form a resulting source identification value;

applying a transformation routine to the resulting source identification value to form a second packet header field; and

storing the second packet header field in the transmit buffer.

[c40] The method for providing trusted communications of claim 33 wherein the step of reforming the transformed packet header comprises the steps of:

extracting a key index value from a packet header field; and

storing the key index value in a first buffer for use throughout the communications session between the source device and the destination device.

[c41] The method for providing trusted communications of claim 40 wherein the step of reforming the transformed packet header further comprises the steps of:

using the key index value to reform another packet header field;

storing a value resulting from the reformed another packet header field in a transmit buffer.

[c42] The method for providing trusted communications of claim 41 further comprising the steps of setting the packet header field to a zero value and storing the zero value in the packet header field in the transmit buffer.

[c43] The method for providing trusted communications of claim 42 further comprising the steps of applying the key index value to the packet header field

and the another packet header field to transform the packet header.

[c44] The method for providing trusted communications of claim 33 further comprising the step of inspecting each received packet to determine if the received packet is a synchronization packet.

[c45] The method for providing trusted communications of claim 44 further comprising the step of determining if the packet header has been transformed by the source device.

[c46] The method for providing trusted communications of claim 45 further comprising the steps of terminating the request for the communications session, reporting the termination of the request in a message to a network administrator and storing the message in an unauthorized event database.

[c47] The method for providing trusted communications of claim 33 further comprising the steps performed at the destination device after a communications session is established with a source device of:

receiving a packet at the destination device;

reforming a first packet header field using a previously stored key index value;

storing the reformed first packet header field in a receive buffer;

reforming a second packet header field using the key index value;

storing the reformed packet header filed in the receive buffer; and

processing the received packet with reformed first and second packet header fields.

[c48] The method for providing trusted communications of claim 47 further comprising the steps of:

transforming the first and second reformed packet header fields;

storing the transformed first and second packet header fields in a transmit buffer; and

transmitting a response packet to the source device including the transformed first and second packet header fields.

[c49] A method for providing trusted communications in a communications network

comprising the steps of:

receiving a synchronization packet with a transformed packet header from a source device;

authenticating the received packet by examination of the transformed packet header; and

releasing the received packet to the destination device if the received packet is authenticated.

[c50] The method for providing trusted communications of claim 49 further comprising the steps of:

inspecting each received packet to determine a corresponding transport protocol;

determining if the received packet is a synchronization packet; and

retaining the received packet for further processing if the received packet is a synchronization packet.

[c51] The method for providing trusted communications of claim 50 further comprising the step of releasing the received packet if it does not match a selected protocol type.

[c52] The method for providing trusted communications of claim 50 further comprising the step of releasing the received packet if it is not a synchronization packet.

[c53] The method for providing trusted communications of claim 49 wherein the step of authenticating the received packet comprises the steps of:

determining if the received packet originated from a trusted source device; and

executing an exception module if the received packet originated from an untrusted source device.

[c54] The method for providing trusted communications of claim 49 wherein the step of authenticating the received packet comprises the steps of:

determining if the received packet originated from a trusted source device;

determining if the packet header has been transformed by the source device;

extracting a determined source identification value and an associated source user identification from the transformed packet header; and

inspecting the packet header to determine if an access policy is specified for the source device.

[c55] The method for providing trusted communications of claim 54 further comprising the steps of determining if a hardware policy is defined and identifying the source device requesting a communications session with a destination device.

[c56] The method for providing trusted communications of claim 54 further comprising the steps of determining if an application policy is defined and verifying a destination port.

[c57] The method for providing trusted communications of claim 54 further comprising the steps of determining if a destination policy is defined and verifying a destination port.

[c58] The method for providing trusted communications of claim 55 further comprising the step of terminating the request for a communication session if either no access policy is specified or if the specified access policy cannot be verified.

[c59] The method for providing trusted communications of claim 58 further comprising the step of reporting the termination of the request for the communications session to a network administrator and storing the message in an unauthorized event database.

[c60] The method for providing trusted communications of claim 53 wherein the step of executing an exception routine comprises the steps of:

extracting an address of the source device from the received packet;

determining if the source device address is an address known to the communications network;

extracting an address of the destination device from the header of the

received packet;

determining if the destination device address is an address known to the communications network;

extracting a port number of the destination device from the header of the received packet; and

determining if the destination port number is known to the communications network.

[c61] The method for providing trusted communications of claim 60 wherein the request for the communications session is terminated if any one of the source node address, the destination node address and the destination port number are not known to the communications network.

[c62] The method for providing trusted communications of claim 60 wherein the step of executing an exception routine further comprises the steps of:

generating an initial value for a packet header field;

selecting a key index value from an array of key index values;

appending the key index value to the generated initial value;

applying the key index value to the generated initial value and appended key index value to form a new transformed packet header field; and

reassembling the received packet including the new transformed packet header field.

[c63] The method for providing trusted communications of claim 62 further comprising the step of determining a checksum value for the new transformed packet header before releasing the received packet to the destination device.

[c64] An appliance for providing trusted communications in a communications network, comprising:

a component for receiving a plurality of packets including transformed packet headers from a client device;

a component for authenticating the plurality of received packets by examination of the transformed packet headers; and

a component for releasing authenticated packets to another

client device.

[c65] The appliance for providing trusted communications of claim 64 wherein the appliance is a standalone network device.

[c66] The appliance for providing trusted communications of claim 64 wherein the appliance is integrated into a network device.

[c67] The appliance for providing trusted communications of claim 64 further comprising:

a component for inspecting each received packet to determine a corresponding transport protocol; and

a component for determining if each received packet is a synchronization packet.

[c68] The appliance for providing trusted communications of claim 64 wherein the authentication component comprises

a component for determining if the received packet originated from a trusted client device; and

a component for executing an exception routine if the received packet originated from an untrusted client device.

[c69] The appliance for providing trusted communications of claim 64 further comprising:

a component for determining if the received packet originated from a trusted client device;

a component for determining if the packet header has been transformed by the client device;

a component for extracting a determined client device identification value and an associated user identification from the transformed packet header; and

a component for inspecting the packet header to determine if an access policy is specified for the client device.

[c70] The appliance for providing trusted communications of claim 6 69 further comprising a component for determining if a hardware policy is defined and

identifying the client device requesting a communications session with another client device.

[c71] The appliance for providing trusted communications of claim 6 69 further comprising a component for determining if an application policy is defined and verifying a destination port.

[c72] The appliance for providing trusted communications of claim 6 69 further comprising a component for determining if a destination policy is defined and verifying a destination port.

[c73] The appliance for providing trusted communications of claim 6 69 further comprising a component for terminating the request for a communication session if either no access policy is specified or if the specified access policy cannot be verified.

[c74] The appliance for providing trusted communications of claim 7 73 further comprising a component for reporting the termination of the request for the communications session to a network administrator and storing the message in an unauthorized event database.

[c75] The appliance for providing trusted communications of claim 6 68 wherein the component for executing an exception routine comprises:

a component for extracting an address of the client device from the received packet;

a component for determining if the client device address is an address known to the communications network;

a component for extracting an address of another client device from the header of the received packet;

a component for determining if the another client device address is an address known to the communications network;

a component for extracting a port number of the another client device from the header of the received packet; and

a component for determining if the another client device port number is known to the communications network.

[c76] The appliance for providing trusted communications of claim 75 wherein the component for executing an exception routine further comprises:

a component for generating an initial value for a packet header field;

a component for selecting a key index value from an array of key index values;

a component for appending the key index value to the generated initial value;

a component for applying the key index value to the generated initial value and appended key index value to form a new transformed packet header field; and

a component for reassembling the received packet including the new transformed packet header field.

[c77] The appliance for providing trusted communications of claim 7 76 urther comprising a component for determining a checksum value for the new transformed packet header before releasing the received packet to the another client device.

[c78] A client device for providing trusted communications in a communications network, comprising:

a component for initiating a request for a communications session;

a component for constructing a transformed packet header for transmission in a synchronization packet to a network device;

a component for receiving a plurality of packets including transformed packet headers from a network device;

a component for reforming transformed packet headers received from a network device; and

a component for constructing a transformed packet header for transmission with an acknowledgement response to the network device.

[c79] The client device for providing trusted communications of claim 7 78 further comprising a component for authenticating identification of the client device by comparing a previously stored value with an identification value determined for the client device.

[c80] The client device for providing trusted communications of claim 7 79 wherein the previously stored value and the determined identification value are based on a hardware address of the client device and an associated user identification.

[c81] The client device for providing trusted communications of claim 7 79 wherein the request for a communications session is terminated if the determined identification value does not match the previously stored value.

[c82] The client device for providing trusted communications of claim 8 80 further comprising a component for reporting the termination of the request for a communications session in a message to a network administrator and storing the message in an unauthorized event database.

[c83] The client device for providing trusted communications of claim 78 wherein the component for constructing a transformed packet header comprises:

a component for selecting a key index value from a first array of key index values;

a component for applying the selected first array key index value to transform a user identification;

a component for appending the first array key index value to the transformed user identification;

a component for selecting a key index value from a second array of index values;

a component for applying the second array key index value to the transformed user identification and appended first array key index value to form a first packet header field; and

a component for storing the first packet header field in a transmit buffer.

[c84] The client device for providing trusted communications of claim 8 83 wherein the component for constructing a transformed packet header further comprises:

a component for appending the second array key index value to a determined identification value to form a resulting identification value;

a component for applying a transformation routine to the resulting identification value to form a second packet header field; and

a component for storing the second packet header field in the transmit buffer.

[c85] The client device for providing trusted communications of claim 78 wherein the component for reforming the transformed packet header comprises:

a component for extracting a key index value from a packet header field; and

a component for storing the key index value in a first buffer for use throughout the communications session with the network device.

[c86] The client device for providing trusted communications of claim 78 wherein the component for reforming the transformed packet header further comprises:

a component for using the key index value to reform another packet header field;

a component for storing a value resulting from the reformed another packet header field in a transmit buffer.

[c87] The client device for providing trusted communications of claim 8 86 further comprising a component for setting the packet header field to a zero value and storing the zero value in the packet header field in the transmit buffer.

[c88] The client device for providing trusted communications of claim 8 87 further comprising a component for applying the key index value to the packet header field and the another packet header field to transform the packet header.

[c89] The client device for providing trusted communications of claim 7 78 further comprising a component for inspecting each received packet to determine if the received packet is a synchronization packet.

[c90] The client device for providing trusted communications of claim 8 89 further comprising a component for determining if the packet header has been transformed by the network device.

[c91] The client device for providing trusted communications of claim 9 90 urther comprising a component for terminating the request for the communications session, reporting the termination of the request in a message to a network

administrator and storing the message in an unauthorized event database.

[c92] A computer readable medium containing a computer program product for providing trusted communication sin in a communications network, comprising:

program instructions that receive a plurality of packets including transformed packet headers from a client device;

program instructions that authenticate the plurality of received packets by examination of the transformed packet headers; and

program instructions that release authenticated packets to another client device.

[c93] The computer program product for providing trusted communications of claim 9 92 urther comprising:

program instructions that inspect each received packet to determine a corresponding transport protocol; and

program instructions that determine if each received packet is a synchronization packet.

[c94] The computer program product for providing trusted communications of claim 92 wherein the program instructions that authenticate comprise:

program instructions that determine if the received packet originated from a trusted client device; and

program instructions that execute an exception routine if the received packet originated from an untrusted client device.

[c95] The computer program product for providing trusted communications of claim 92 wherein the program instructions that authenticate, further comprise:

program instructions that determine if the received packet originated from a trusted client device;

program instructions that determine if the packet header has been transformed by the client device;

program instructions that extract a determined client device identification value and an associated user identification from the packet header; and

program instructions that inspect the packet header to determine if an access policy is specified for the client device.

[c96] The computer program product for providing trusted communications of claim 9 95 further comprising program instructions that determine if a hardware policy is defined and identify the client device requesting a communications session with another client device.

[c97] The computer program product for providing trusted communications of claim 9 95 further comprising a program instructions that determine if an application policy is defined and verify a destination port.

[c98] The computer program product for providing trusted communications of claim 9 95 urther comprising program instructions that determine if a destination policy is defined and verify a destination port.

[c99] The computer program product for providing trusted communications of claim 9 95 urther comprising program instructions that terminate the request for a communication session if either no access policy is specified or if the specified access policy cannot be verified.

[c100] The computer program product for providing trusted communications of claim 9 99 further comprising program instructions that report the termination of the request for the communications session to a network administrator and store the message in an unauthorized event database.

[c101] The computer program product for providing trusted communications of claim 9 94 wherein the program instructions that execute an exception routine comprise:

program instructions that extract an address of the client device from the received packet;

program instructions that determine if the client device address is an address known to the communications network;

program instructions that extract an address of another client device from the header of the received packet;

program instructions that determine if the another client device address is an address known to the communications network;

program instructions that extract a port number of another client device

from the header of the received packet; and

program instructions that determine if the another client device port number is known to the communications network.

[c102] The computer program product for providing trusted communications of claim 1 101 wherein the program instructions that execute an exception routine further comprise::

program instructions that select a key index value from an array of key index values;

program instructions that append the key index value to the generated initial value;

program instructions that apply the key index value to the generated initial value and appended key index value to form a new transformed packet header field; and

program instructions that reassemble the received packet including the new transformed packet header field.

[c103] The computer program product for providing trusted communications of claim 1 102 further comprising program instructions that determine a checksum value for the new transformed packet header before releasing the received packet to the another client device.

[c104] A computer readable medium containing a computer program product for providing trusted communications in a communications network, comprising:

program instructions that initiate a request for a communications session;

program instructions that construct a transformed packet header for transmission in a synchronization packet to a network device;

program instructions that receive a plurality of packets including transformed packet headers from a network device;

program instructions that reform transformed packet headers received from a network device; and

program instructions that construct a transformed packet header for transmission with an acknowledgement response to the network device.

[c105] The computer program product for providing trusted communications of claim

1 104 further comprising program instructions that authenticate identification of the client device by comparing a previously stored value with an identification value determined by the client device.

[c106] The computer program product for providing trusted communications of claim 1 105 wherein the previously stored value and the determined identification value are based on a hardware address of the client device and an associated user identification.

[c107] The computer program product for providing trusted communications of claim 1 105 wherein the request for a communications session is terminated if the determined identification value does not match the previously stored value.

[c108] The computer program product for providing trusted communications of claim 1 106 further comprising program instructions that report the termination of the request for a communications session in a message to a network administrator and store the message in an unauthorized event database.

[c109] The computer program product for providing trusted communications of claim 1 104 wherein the program instructions that construct a transformed packet header comprise:

program instructions that select a key index value from a first array of key index values;

program instructions that apply the selected first array key index value to transform a user identification;

program instructions that append the first array key index value to the transformed user identification;

program instructions that select a key index value from a second array of index values;

program instructions that apply the second array key index value to the transformed user identification and appended first array key index value to form a first packet header field; and

program instructions that store the first packet header field in a transmit buffer.

[c110] The computer program product for providing trusted communications of claim 1 109 wherein the program instructions that construct a transformed packet header further comprise:

program instructions that append the second array key index value to a determined identification value to form a resulting identification value;

program instructions that apply a transformation routine to the resulting identification value to form a second packet header field; and

program instructions that store the second packet header field in the transmit buffer.

[c111] The computer program product for providing trusted communications of claim 1 104 wherein the program instructions that reform the transformed packet header comprise:

program instructions that extract a key index value from a packet header field; and

program instructions that store the key index value in a first buffer for use throughout the communications session with the network device.

[c112] The computer program product for providing trusted communications of claim 1 104 wherein the program instructions that reform the transformed packet header further comprise:

program instructions that use the key index value to reform another packet header field; and

program instructions that store a value resulting from the reformed another packet header field in a transmit buffer.

[c113] The computer program product for providing trusted communications of claim 1 112 further comprising program instructions that set the packet header field to a zero value and store the zero value in the packet header field in the transmit buffer.

[c114] The computer program product for providing trusted communications of claim 1 113 further comprising program instructions that apply the key index value to the packet header field and the another packet header field to transform the packet header.

[c115] The computer program product for providing trusted communications of claim 1 104 urther comprising program instructions that inspect each received packet to determine if the received packet is a synchronization packet.

[c116] The computer program product for providing trusted communications of claim 1 115 further comprising program instructtionsthat determine if the packet header has been transformed by the network device.

[c117] The computer program product for providing trusted communications of claim 1 116 further comprising program instructions that terminate the request for the communications session, report the termination of the request in a message to a network administrator and store the message in an unauthorized event database.